Counting homomorphisms onto finite solvable groups

Daniel Matei [a,b] Alexander I. Suciu [b,1]

[a]*Institute of Mathematics of the Academy, P.O. Box 1-764, RO-014700 Bucharest, Romania*

[b]*Department of Mathematics, Northeastern University, Boston, MA 02115*

Abstract

We present a method for computing the number of epimorphisms from a finitely presented group G to a finite solvable group Γ, which generalizes a formula of Gaschütz. Key to this approach are the degree 1 and 2 cohomology groups of G, with certain twisted coefficients. As an application, we count low-index subgroups of G. We also investigate the finite solvable quotients of the Baumslag-Solitar groups, the Baumslag parafree groups, and the Artin braid groups.

Key words: Solvable quotients, chief series, Gaschütz formula, group cohomology, finite-index subgroups, Baumslag-Solitar groups, parafree groups, braid groups

2000 Mathematics Subject Classification: Primary 20J05, 20F16; Secondary 20E07, 20F36, 57M05.

1 Introduction

1.1 Finite quotients

One way to understand an infinite, finitely generated group is to identify its finite quotients, and count all the epimorphisms to one of these finite groups. A wide spectrum of possibilities can occur. For example, residually finite groups have plenty of finite quotients, whereas infinite simple groups have none. Free

---

groups and surface groups have an abundance of finite solvable quotients, whereas groups with perfect derived subgroup have no solvable quotients except abelian ones.

If G is a finitely generated group, and Γ a finite group, let $|\mathrm{Hom}(G,\Gamma)|$ be the number of homomorphisms from G to Γ, and let $\delta_\Gamma(G) = |\mathrm{Epi}(G,\Gamma)|\,/\,|\mathrm{Aut}\,\Gamma|$ be the number of epimorphisms from G to Γ, up to automorphisms of Γ. In the case when $G = F_n$ is the free group of rank n, Philip Hall [15] gave a procedure to determine the Eulerian function $|\mathrm{Epi}(F_n,\Gamma)|$, based on Möbius inversion in the subgroup lattice of Γ. An explicit formula for computing $|\mathrm{Epi}(F_n,\Gamma)|$ in the case when Γ is solvable was given by Gaschütz [11].

In this paper, we generalize Gaschütz's formula, from the free group F_n, to an arbitrary finitely presented group G. As a byproduct, we derive an expression for the order of the automorphism group of a finite solvable group Γ. Putting things together gives a method for computing the solvable Hall invariants $\delta_\Gamma(G)$ in terms of homological data. This extends previous results from [26], which only dealt with certain metabelian groups Γ.

1.2 Finite-index subgroups

Another way to understand a finitely generated, residually finite group is through its finite-index subgroups. Let $a_k(G)$ and $a_k^\triangleleft(G)$ be the number of index k subgroups (respectively, normal subgroups) of G. The growth of these sequences—also known as the subgroup growth of G—has been a subject of intensive study in the recent past, see [25]. Much is known in the case when G is nilpotent; explicit formulas for $a_k(G)$ and $a_k^\triangleleft(G)$ are available in a few other cases, such as free products of cyclic groups and surface groups.

In [14], Marshall Hall showed how to express the numbers $a_k(G)$ in terms of the Hall invariants $\delta_\Gamma(G)$, where Γ ranges through the isomorphism classes of subgroups of the symmetric group S_k. In [26], we used this fact to arrive at a homological formula for $a_3(G)$. Here, we give a similar (but more involved) formula for $a_4(G)$. Combining our previous results with the present techniques, we also give formulas for $a_k^\triangleleft(G)$, for $k \leq 15$.

1.3 Solvable quotients

The derived series of a group G is defined inductively by $G^{(0)} = G$ and $G^{(k)} = [G^{(k-1)}, G^{(k-1)}]$. A group G is solvable if its derived series terminates. The derived length of G is the minimal k for which $G^{(k)} = 1$; abelian groups have derived length 1, while metabelian groups have length 2.

2

At the other extreme, a perfect group G equals its own derived subgroup, so its derived series stabilizes at $G' = G^{(1)}$. Clearly, a solvable group has no perfect subgroups. Hence, if $G^{(k)}$ is perfect, then G has no solvable quotients of derived length greater than k.

Now suppose Γ is a finite solvable group, of derived length l. Since the derived series of G consists of characteristic subgroups, the number of epimorphisms from G to Γ depends only on the solvable quotient $G/G^{(l)}$; in fact, $|\mathrm{Epi}(G, \Gamma)| = |\mathrm{Epi}(G/G^{(l)}, \Gamma)|$.

1.4   Lifting homomorphisms

As is well-known, a group is solvable if and only if it can be expressed as an iterated extension of abelian groups. In order to count homomorphisms from a finitely generated group G to a finite solvable group Γ, we use an inductive procedure, sketched below.

Suppose we have an extension $1 \to A \to \Gamma \to B \to 1$, with A abelian and B solvable. Such an extension is determined by a monodromy homomorphism $\sigma \colon B \to \mathrm{Aut}(A)$, and a (twisted) cohomology class $[\chi] \in H^2_\sigma(B, A)$. Let $\rho \colon G \to B$ be a homomorphism. Then ρ has a lift $\tilde\rho \colon G \to \Gamma$ if and only if $\rho^*[\chi] = 0$ in $H^2_{\sigma\rho}(G, A)$. Furthermore, the lifts of ρ are in one-to-one correspondence with 1-cochains that cobound the 2-cocycle $-\rho^*\chi$. The set of such 1-cochains, $Z^1_{\sigma\rho, \chi}(G, A)$, is either empty, or is in bijection with $Z^1_{\sigma\rho}(G, A)$; define $\epsilon_\chi(\rho)$ to be 0 or 1, accordingly. We find:

$$|\mathrm{Hom}(G, \Gamma)| = \sum_{\rho \in \mathrm{Hom}(G, B)} \epsilon_\chi(\rho) \cdot \left| Z^1_{\sigma\rho}(G, A) \right|.$$

1.5   Systems of equations

If G admits a finite presentation, say $\mathcal{P} = \langle x_1, \dots, x_n \mid r_1, \dots, r_m \rangle$, we can translate the lifting condition into a system $S = S(\mathcal{P}, \Gamma, \rho)$ of m equations in n unknowns over the abelian group A. The equations in S, given in (3.4) below, are similar in nature to inhomogeneous linear equations. The homogeneous part is written in terms of the Fox derivatives $\partial r_i/\partial x_j$, twisted by $\sigma\rho$, whereas the non-homogeneous part involves only $\rho^*\chi$ and the presentation $\mathcal{P}$.

As shown in Theorem 3.4, the number of solutions of the system S coincides with the number of lifts of ρ. The precise determination of these solutions gives a way to explicitly construct those lifts.

In general, the system of equations S cannot be reduced to a linear system. But, in certain cases, this is possible. One instance (exploited in [9] and [26]) is when B is abelian, A is the additive group of a finite commutative ring R, and σ is induced by multiplication in R. Another instance is when A is homo-cyclic, say $A = \mathbb{Z}_{q^r}^{\oplus s}$, and the monodromy is of the form $\sigma \colon B \to \mathrm{GL}(s, \mathbb{Z}_{q^r})$. In particular, if A is an elementary abelian q-group E, the cohomology group $H^1(G, E)$ can be viewed as a vector space over the prime field $\mathbb{Z}_q$, and its dimension can be computed in terms of the rank of the Jacobian matrix associated to a presentation of G, twisted by the homomorphism ρ.

1.6 A generalization of Gaschütz' formula

Next, we restrict our attention to surjective homomorphisms $G \twoheadrightarrow \Gamma$. From the above discussion, we know that $|\mathrm{Hom}(G, \Gamma)|$ can be obtained by summing $\epsilon_\chi(\rho) q^{\dim_{\mathbb{Z}_q} Z^1_{\sigma\rho}(G,E)}$ over all $\rho \in \mathrm{Hom}(G, B)$. In order to compute $|\mathrm{Epi}(G, \Gamma)|$, we have to subtract all the homomorphisms $G \to \Gamma$ which are not surjective. Due to the minimality of E, those are precisely the homomorphisms whose image is a complement of E in Γ.

Every solvable group Γ admits a normal series whose successive factors are elementary abelian. Our method for calculating $|\mathrm{Epi}(G, \Gamma)|$ is to use such a chief series to construct all the epimorphisms by repeated liftings through the chief series. The key step is provided by the following result.

Theorem *Let G be a finitely presented group, and let Γ be a finite, solvable group. Let E be an elementary abelian q-group which is also a chief factor of Γ, and let $B = \Gamma/E$. If σ is the monodromy and χ is the 2-cocycle defining the extension $1 \to E \to \Gamma \to B \to 1$, then:*

$$|\mathrm{Epi}(G, \Gamma)| = |E|^\zeta \sum_{\rho \in \mathrm{Epi}(G,B)} \left(\epsilon_\chi(\rho) q^{\dim_{\mathbb{Z}_q} H^1_{\sigma\rho}(G,E)} - c_\chi q^{\kappa(\alpha-1)} \right),$$

where $\zeta = 0$ or 1 according as B acts trivially on E or not, $\epsilon_\chi(\rho) = 1$ or 0 according as the equation $\delta^1 f = -\rho^*\chi$ has a solution or not, $c_\chi = 1$ or 0 according as $[\chi] \in H^2_\sigma(B, E)$ vanishes or not, α is the number of complemented chief factors of Γ isomorphic to E as Γ-modules (under the conjugation action), and $q^\kappa = |\mathrm{End}_\Gamma(E)|$.

Now suppose $\Gamma = \Gamma_0 > \Gamma_1 > \cdots > \Gamma_\nu > \Gamma_{\nu+1} = 1$ is a chief series, with factors $E_i = \Gamma_i/\Gamma_{i+1} = \mathbb{Z}_{q_i}^{\oplus s_i}$ and quotients $B_i = \Gamma/\Gamma_i$. We then find:

$$|\mathrm{Epi}(G, \Gamma)| = \sum_{\rho_1 \in \mathrm{Epi}_{\rho_0}(G,B_1)} \cdots \sum_{\rho_\nu \in \mathrm{Epi}_{\rho_{\nu-1}}(G,B_\nu)} |E_\nu|^{\zeta_\nu} \left(\epsilon_{\chi_\nu}(\rho_\nu) q_\nu^{\beta_\nu} - c_{\chi_\nu} q_\nu^{\kappa_\nu(\alpha_\nu-1)} \right),$$

where $B_{\nu+1} = E_\nu \times_{\sigma_\nu, \chi_\nu} B_\nu$, $\beta_\nu = \dim_{\mathbb{Z}_{q_\nu}} H^1_{\sigma_\nu\rho_\nu}(G, E_\nu)$, let α_ν be the number

of chief factors of $B_{\nu+1}$ isomorphic to E_ν as $B_{\nu+1}$-modules, and $\mathrm{Epi}_{\rho_i}(G, B_{i+1})$ is the set of epimorphisms lifting $\rho_i \colon G \twoheadrightarrow B_i$. In the case when $G = F_n$, this recovers Gaschütz' formula.

1.7   Examples

To illustrate our recursive process for calculating $|\mathrm{Epi}(G, \Gamma)|$, we discuss various classes of source and target groups.

When it comes to the target group Γ, we analyze in detail two series of finite metabelian groups: the dihedral and the binary dihedral groups. We also consider a class of derived length 3 solvable groups, of the form $\Gamma = \mathbb{Z}_q^2 \rtimes D_{2p}$, which includes the symmetric group $S_4 = \mathbb{Z}_2^{\oplus 2} \rtimes D_6$.

In calculating $|\mathrm{Epi}(G, \Gamma)|$, one can use the lattice of subgroups of Γ instead of its chief series extensions. We briefly illustrate this approach for the sake of comparison, in the case when Γ is a dihedral group.

When it comes to the source group G, we start of course with the free groups F_n. Another family of examples are the orientable and non-orientable surface groups, Π_g and Π_g^*. The other examples we consider (the one-relator Baumslag-Solitar and Baumslag groups, a certain link group, and the Artin braid groups) are discussed separately below.

1.8   Baumslag-Solitar groups

A famous family of one-relator groups was introduced by Baumslag and Solitar in [4]. For each pair of integers (m, n) with $0 < m \le |n|$, let $\mathrm{BS}(m, n) = \langle x, y \mid xy^m x^{-1} y^{-n} \rangle$. Much is known about these groups: $\mathrm{BS}(m, n)$ is solvable if and only if $m = 1$, in which case $\mathrm{BS}(1, n) = \mathbb{Z}[1/n] \rtimes \mathbb{Z}$; it is residually finite if and only if $m = |n|$ or $m = 1$, in which case it is also Hopfian; and it is Hopfian if and only if m and n have the same prime divisors or $m = 1$. For example, $\mathrm{BS}(2, 3)$ is non-Hopfian, while $\mathrm{BS}(2, 4)$ is Hopfian but non-residually finite.

The groups $\mathrm{BS}(m, n)$ have been classified by Moldavanski [27]. They are in bijection with the set of unordered pairs (m, n) with $0 < m \le |n|$. In the case when $m = 1$, the set of finite quotients of $\mathrm{BS}(1, n)$ is a complete group invariant, see [28], and it consists of all quotients of metacyclic groups of type $\mathbb{Z}_s \rtimes_\sigma \mathbb{Z}_r$, where σ is multiplication by n, and $n^r \equiv 1 \pmod s$. The subgroup growth of the Baumslag-Solitar groups $\mathrm{BS}(m, n)$, with m, n coprime was determined by E. Gelman, see [25, p. 284]; a presentation for $\mathrm{Aut}(\mathrm{BS}(m, n))$ was given in [12].

We compute here the number of epimorphisms from the Baumslag-Solitar groups to D_8 and Q_8. This allows us to divide the groups $\mathrm{BS}(m,n)$ into four (respectively, two) non-isomorphic classes.

1.9 Baumslag's parafree groups

In [3], Baumslag introduced the following notion: A group G is called parafree if it is residually nilpotent and has the same nilpotent quotients as a free group F. The simplest non-free yet parafree groups are the one-relator groups $P(m,n) = \langle x, y, z \mid xz^m xz^{-m} x^{-1} z^n yz^{-n} y^{-1} \rangle$. As shown in [3], each group in this family (indexed by pairs of integers m and n) has the same nilpotent quotients and the same first two solvable quotients as the free group F_2.

In [21], R. Lewis and S. Liriano showed that there are several distinct isomorphism types among the groups $P(m,n)$. By counting homomorphisms to $\mathrm{SL}(2,\mathbb{Z}_4)$, they verified that the third solvable quotients of $P(m,n)$ differ from those of F_2, for certain pairs of integers, e.g., $(m,n) = (1,3)$ and $(3,5)$. By computing the number of epimorphisms of $P(m,n)$ onto a smaller solvable quotient group of derived length 3, namely S_4, we can recover (and sharpen) the result of Lewis and Liriano. We find: If m odd and $m - n \equiv 2 \pmod 4$, then $P(m,n)$ is not isomorphic to F_2. Moreover, in that case, $P(m,n)$ is not isomorphic to $P(m',n')$ if m' even or $m' - n' \not\equiv 2 \pmod 4$.

1.10 A link group

Counting finite solvable quotients of a group G can also help decide whether a normal subgroup H is perfect. Indeed, if $H \triangleleft G$ is perfect, and Γ is finite and solvable, then $\delta_\Gamma(G) = \delta_\Gamma(G/H)$. In other words, if $\delta_\Gamma(G) > \delta_\Gamma(G/H)$ for some finite solvable group Γ, then H is not perfect.

As an example of how this works, we take G to be the group of a certain 2-component link considered by Hillman in [16]. Then G_ω, the intersection of the lower central series of G, is non-trivial, i.e., G is not residually nilpotent. Hence, G is not parafree. On the other hand, $G/G_\omega \cong P(-1,1)$, and thus G has the same nilpotent quotients as F_2; moreover, $G/G'' \cong F_2/F_2''$. Using our formula, we find that $\delta_{S_4}(G) > \delta_{S_4}(P(-1,1))$. This shows that G_ω is not perfect, thereby answering a question of Hillman, see [16, p. 74].

The braid groups B_n have been intensively studied ever since Artin introduced them in the mid 1920's. Although the braid groups are residually finite, few of their finite quotients are known. General series of non-abelian quotients for B_n ($n \geq 3$) are the symmetric groups S_n, and the projective symplectic groups $\mathrm{PSp}(n-2,3)$ with n even, or $\mathrm{PSp}(n-1,3)$ with n odd.

Once we restrict to solvable quotients, the situation becomes more manageable. In Section 10 we use our methods to compute the number of epimorphisms from B_n to certain finite solvable groups. For example, we show that $\delta_{S_3}(B_3) = 1$ and $\delta_{S_4}(B_4) = 3$ (this recovers a particular case of a much more general result of Artin [1], see also [6]). Using results of V. Lin, we also compute the number of index k subgroups of B_n, when $k \leq n$ or $k = 2n$, and n is sufficiently large.

We conclude with some conjectures on the possible values for $\delta_\Gamma(B_n)$, for solvable Γ, and on the behavior of the sequence $a_k(B_n)$, for $n \gg 0$.

2   Extensions and group cohomology

In this section, we review some basic material on group cohomology. We outline a computation method based on Fox calculus, and explain how low-degree cohomology is connected with extensions with abelian kernel. We use [5] and [17] as general reference.

2.1   Group cohomology and Fox calculus

Let G be a group, and A a G-module, with action specified by a homomorphism $\alpha \colon G \to \mathrm{Aut}(A)$. Let $C^r = \mathrm{Maps}(G^{\times r}, A)$ be the group of r-cochains, and define coboundary maps $\delta^r \colon C^r \to C^{r+1}$ by $\delta^r(f)(x_0, \ldots, x_r) = x_0 f(x_1, \ldots, x_r) - \sum_{i=0}^{r-1}(-1)^i f(x_0, \ldots, x_i x_{i+1}, \ldots, x_r) + (-1)^{r-1} f(x_0, \ldots, x_{r-1})$. The cohomology groups of G with coefficients in A are defined as

$$H_\alpha^r(G, A) = Z_\alpha^r(G, A)/B_\alpha^r(G, A), \tag{2.1}$$

where $Z_\alpha^r(G, A) = \ker(\delta^r)$ are the cocycles and $B_\alpha^r(G, A) = \mathrm{im}(\delta^{r-1})$ are the coboundaries.

Now suppose G admits a finite presentation, $G = F_n/R$, where F_n is the free group on $x_1, \ldots, x_n$ and R is the normal subgroup generated by $r_1, \ldots, r_m$. The

Fox derivatives $\frac{\partial}{\partial x_j} \colon \mathbb{Z}F_n \to \mathbb{Z}F_n$ are the $\mathbb{Z}$-linear maps defined by $\frac{\partial x_i}{\partial x_j} = \delta_{ij}$ and $\frac{\partial(uv)}{\partial x_j} = \frac{\partial u}{\partial x_j}\epsilon(v) + u\frac{\partial v}{\partial x_j}$, where $\epsilon\colon \mathbb{Z}F_n \to \mathbb{Z}$ is the augmentation map. The beginning of a free resolution of $\mathbb{Z}$ by $\mathbb{Z}G$-modules is then

$$\mathbb{Z}G^m \xrightarrow{J_G} \mathbb{Z}G^n \xrightarrow{d_1} \mathbb{Z}G \xrightarrow{\epsilon} \mathbb{Z} \longrightarrow 0 \,, \tag{2.2}$$

where $d_1 = \phi(x_1 - 1 \ldots x_n - 1)^\top$ and $J_G = \phi\left(\partial r_i/\partial x_j\right)$ is the Fox Jacobian matrix. Applying $\mathrm{Hom}_{\mathbb{Z}G}(-, A)$ yields the cochain complex

$$A \xrightarrow{d_1^\alpha} A^n \xrightarrow{J_G^\alpha} A^m \,, \tag{2.3}$$

whose homology is $H_\alpha^1(G, A)$.

2.2 Extensions with abelian kernel

An extension Γ of a group B by an abelian group A (written additively) is a short exact sequence

$$1 \longrightarrow A \xrightarrow{i} \Gamma \xrightarrow{\pi} B \longrightarrow 1 \,, \tag{2.4}$$

determined by:

- the monodromy homomorphism $\sigma\colon B \to \mathrm{Aut}(A)$, defined by $i(\sigma_b(a)) = s(b) \cdot i(a) \cdot s(b)^{-1}$, where $s\colon B \to \Gamma$ is any set section of π;
- the cohomology class $[\chi] \in H_\sigma^2(B, A)$ of a normalized 2-cocycle $\chi\colon B \times B \to A$, defined by $i(\chi(b, b')) = s(b)s(b')s(bb')^{-1}$.

An element of Γ can we written as a pair (a, b) with $a \in A$ and $b \in B$, while multiplication in Γ is given by $(a_1, b_1) \cdot (a_2, b_2) = (a_1 + \sigma_{b_1}(a_2) + \chi(b_1, b_2), b_1 b_2)$. Note that $(a, b)^{-1} = (-\sigma_{b^{-1}}(a) - \chi(b^{-1}, b), b^{-1})$.

We denote a group Γ as in (2.4) by $\Gamma = A \times_{\sigma,\chi} B$. In the case of a split extension $([\chi] = 0)$, we simply write $\Gamma = A \rtimes_\sigma B$; in the case of a central extension $(\sigma_b = \mathrm{id}$, for all $b \in B)$, we write $\Gamma = A \times_\chi B$.

Now assume $\Gamma = A \times_{\sigma,\chi} B$ is finite, and let $c(\Gamma)$ be the number of complements of A in Γ. If the extension splits (which we write as $c_\chi = 1$), then $c(\Gamma) = |Z_\sigma^1(B, A)|$; if the extension does not split (which we write as $c_\chi = 0$), then $c(\Gamma) = 0$. Thus:

$$c(\Gamma) = c_\chi \left| Z_\sigma^1(B, A) \right| . \tag{2.5}$$

3 Lifting homomorphisms

In this section, we present a method for counting the homomorphisms from a finitely presented group G to a finite group Γ, given as an extension with abelian kernel.

3.1 Homomorphisms into extensions

Let G be a finitely generated group, and $\rho\colon G \to B$ a homomorphism to a group B. Let $\Gamma = A \times_{\sigma,\chi} B$ be an extension of B by an abelian group A, with monodromy $\sigma\colon B \to \mathrm{Aut}(A)$ and 2-cocycle $\chi\colon B \times B \to A$. Then A becomes a G-module, with action specified by $\sigma\rho\colon G \to \mathrm{Aut}(A)$. Let $Z^1_{\sigma\rho}(G, A)$ and $H^1_{\sigma\rho}(G, A)$ be the corresponding 1-cocycle and 1-cohomology groups.

Any set map $\lambda\colon G \to \Gamma$ lifting $\rho\colon G \to B$ can be written as a pair of maps $\lambda = (f, \rho)$, with $f\colon G \to A$. Then λ is a homomorphism if and only if f satisfies the following:

$$f(gh) = f(g) + \sigma_{\rho(g)}(f(h)) + \chi(\rho(g), \rho(h)), \quad \text{for all } g, h \in G, \tag{3.1}$$

that is, f is a 1-cochain that cobounds the 2-cocycle $-\rho^*\chi\colon G \times G \to A$. Denote the set of all such 1-cochains by

$$Z^1_{\sigma\rho,\chi}(G, A) = \{f\colon G \to A \mid \delta^1 f = -\rho^*\chi\}. \tag{3.2}$$

This set is either empty, or else $Z^1_{\sigma\rho,\chi}(G, A) = Z^1_{\sigma\rho}(G, A) + f_0$, for some 1-cochain f_0. Set $\epsilon_\chi(\rho)$ to be 0 or 1, accordingly. We then have the following.

Proposition 3.2 *The number of homomorphisms from G to $\Gamma = A \times_{\sigma,\chi} B$ is given by*

$$\left|\mathrm{Hom}(G, A \times_{\sigma,\chi} B)\right| = \sum_{\rho \in \mathrm{Hom}(G,B)} \epsilon_\chi(\rho) \cdot \left|Z^1_{\sigma\rho}(G, A)\right|. \tag{3.3}$$

If the extension is split, then clearly $\epsilon_0(\rho) = 1$ for all $\rho\colon G \to B$, and thus (3.3) reduces to $|\mathrm{Hom}(G, A \rtimes_\sigma B)| = \sum_\rho \left|Z^1_{\sigma\rho}(G, A)\right|$. If the extension is central, then $Z^1_{\sigma\rho}(G, A) = \mathrm{Hom}(G, A)$ for all ρ, and thus $|\mathrm{Hom}(G, A \times_\chi B)| = \sum_\rho \epsilon_\chi(\rho) |\mathrm{Hom}(G, A)|$. If the extension is both split and central (i.e., a direct product), then (3.3) reduces to the well-known formula $|\mathrm{Hom}(G, A \times B)| = |\mathrm{Hom}(G, A)| \cdot |\mathrm{Hom}(G, B)|$.

3.3 Equations for lifts

We now give a practical algorithm for computing the quantities involved in Formula (3.3), in the case when G is a finitely presented group. Given a homomorphism $\rho \colon G \to B$, we want to decide whether there is a 1-cochain $f \colon G \to A$ cobounding $-\rho^* \chi$ (i.e., whether $\epsilon_\chi(\rho) \neq 0$), and, if so, count how many such cochains there are (i.e., determine $\left| Z^1_{\sigma\rho}(G, A) \right|$).

Let $\mathcal{P} = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_m \rangle$ be a finite presentation for G, and $\phi \colon F_n \to G$ the presenting homomorphism. Write $r_k = u_{k,1} \cdots u_{k,l_k}$, with each $u_{k,j}$ equal to some $x_i^{e_{k,j}}$, where $e_{k,j} = \pm 1$.

Theorem 3.4 *Let $\rho \colon G \to B$ be a homomorphism. Then $\epsilon_\chi(\rho) = 1$ or 0 according to whether the following system of equations has a solution $(a_1, \ldots, a_n)$ with $a_i \in A$:*

$$
\begin{aligned}
\sum_{i=1}^n \sigma\bar\rho\left(\frac{\partial r_k}{\partial x_i}\right)(a_i) + \sum_{j=1}^{l_k} \frac{e_{k,j} - 1}{2} \chi\left(\bar\rho(u_{k,j}), \bar\rho(u_{k,j}^{e_{k,j}})\right) \\
+ \sum_{j=1}^{l_k - 1} \chi\left(\bar\rho(u_{k,1} \cdots u_{k,j}), \bar\rho(u_{k,j+1})\right) = 0, \quad 1 \le k \le m,
\end{aligned}
\tag{3.4}
$$

where $\bar\rho = \rho\phi$. Moreover, if $\epsilon_\chi(\rho) = 1$, then $\left| Z^1_{\sigma\rho}(G, A) \right|$ equals the number of solutions of the (homogeneous) system

$$
\sum_{i=1}^n \sigma\bar\rho\left(\tfrac{\partial r_k}{\partial x_i}\right)(a_i) = 0, \qquad 1 \le k \le m.
\tag{3.5}
$$

PROOF. Let $f \colon G \to A$ be a 1-cochain that cobounds $-\rho^*\chi$. From the cocycle condition (3.1) it follows that $f \colon G \to A$ is uniquely determined by its value on the generators. Now note that the map $\bar f = f\phi \colon F_n \to \Gamma$ vanishes on the relators of G:

$$
\bar f(r_k) = 0, \qquad 1 \le k \le m.
\tag{3.6}
$$

To finish the proof, we need to express this system of equations in terms of the the values $\bar f(x_i) = a_i$, and count the number of solutions.

To that end, let $r = u_1 \cdots u_l$ be a word in F_n, with $u_j = x_{i_j}^{e_j}$. Then the following

10

equality holds in the abelian group A:

$$\bar{f}(r) = \sum_{i=1}^{n} \sigma\bar{\rho}\left(\tfrac{\partial r}{\partial x_i}\right)(a_i) + \sum_{j=1}^{l} \tfrac{e_j-1}{2}\chi\left(\bar{\rho}(u_j), \bar{\rho}(u_j^{e_j})\right) + \tag{3.7}$$
$$\sum_{j=1}^{l-1} \chi\left(\bar{\rho}(u_1 \cdots u_j), \bar{\rho}(u_{j+1})\right).$$

This follows by induction on the length l of the word r, using (3.1). A detailed proof, in the case when $\Gamma = A \rtimes_\sigma B$, is given in [26, Lemma 7.3]. The general case works similarly.

From (3.7), it is apparent that the system of equations (3.6) coincides with (3.4). By definition, the set of solutions to (3.4) equals $Z^1_{\sigma\rho,\chi}(G, A)$. When this set is non-empty (i.e., $\epsilon_\chi(\rho) = 1$), then $\left|Z^1_{\sigma\rho,\chi}(G, A)\right| = \left|Z^1_{\sigma\rho}(G, A)\right|$, cf. §3.1. So it is enough to count solutions of the system (3.4) in the particular case when $[\chi] = 0$. But this system is (3.5), and we are done. $\square$

In particular, if $G = F_n$, then the system (3.4) is empty, and so $\epsilon_\chi(\rho) = 1$, for any homomorphism $\rho\colon F_n \to B$ and extension $\Gamma = A \times_{\sigma,\chi} B$.

3.5   Corank of twisted Jacobian

With notation as in Theorem 3.4, suppose A is an abelian q-group, where q is a prime. Then the number of solutions of system (3.5) is of the form q^d, for some $d \geq 0$. Denote this integer by $d(\sigma\rho)$. Then:

$$\left|Z^1_{\sigma\rho}(G, A)\right| = q^{d(\sigma\rho)}. \tag{3.8}$$

For an arbitrary finite abelian group A, denote by A_q the q-torsion subgroup. Then $A = \bigoplus_{q|\,|A|} A_q$ as G-modules, and $Z^1_{\sigma\rho}(G, A) = \bigoplus_q Z^1_{\pi_q\sigma\rho}(G, A_q)$, where $\pi_q\colon \mathrm{Aut}(A) \to \mathrm{Aut}(A_q)$ is the canonical projection. Hence:

$$\left|Z^1_{\sigma\rho}(G, A)\right| = \prod_{q|\,|A|} q^{d(\pi_q\sigma\rho)}. \tag{3.9}$$

Now assume A is homocyclic, say $A = \mathbb{Z}_{q^r}^{\oplus s}$. Then $\mathrm{Aut}(A)$ can be identified with $\mathrm{GL}(s, \mathbb{Z}_{q^r})$. Thus (3.5) becomes a system of linear equations over the ring $\mathbb{Z}_{q^r}$, and

$$d(\sigma\rho) = \mathrm{corank}\left(J_G^{\sigma\rho}\right). \tag{3.10}$$

Here recall $J_G = \phi\left(\partial r_i/\partial x_j\right)$ is the $m \times n$ matrix over $\mathbb{Z}G$ associated to the presentation $\mathcal{P} = \langle x_1, \ldots, x_n \mid r_1, \ldots, r_m \rangle$ for G, while $J_G^{\sigma\rho}$ is the $ms \times ns$

11

matrix over $\mathbb{Z}_{q^r}$ obtained by replacing each entry e of J_G by the matrix $\sigma\rho(e) \in \mathrm{Aut}(A) = \mathrm{GL}(s, \mathbb{Z}_{q^r})$.

4 Generalized Gaschütz formula

In this section, we give a formula counting the number of epimorphisms from a finitely presented group G to a finite, solvable group Γ. We use [29] as a general reference for group theory.

4.1 Complements in finite solvable groups

A group is said to be *solvable* if its derived series terminates. For a finite group Γ, this is equivalent to Γ having an elementary abelian chief series, i.e., a non-refinable series of normal subgroups, such that all the quotients are elementary abelian. By a classical result, any minimal normal subgroup of Γ must be an elementary abelian group E; moreover, the quotient $B = \Gamma/E$ acts linearly on E.

We will need the following result of Gaschütz.

Theorem 4.2 ([11], Satz 3) *Let $\Gamma = E \times_{\sigma,\chi} B$ be an extension of a finite, solvable group B by an elementary abelian q-group E which is a minimal normal subgroup of Γ. Then the number of complements of E in Γ is given by*

$$c(\Gamma) = c_\chi \cdot |E|^\zeta \cdot q^{\kappa(\alpha-1)}, \tag{4.1}$$

where $c_\chi = 1$ or 0 according as $[\chi] = 0$ or not, $\zeta = 0$ or 1 according as B acts trivially on E or not, and α is the number of complemented chief factors of Γ isomorphic to E as Γ-modules under the conjugation action.

If $c_\chi = 0$, the extension is non-split, and so $c(\Gamma) = 0$; the case $c_\chi = 1$ is the one requiring an argument. The proof in [11] breaks into several steps. First, it is shown that $c(\Gamma) = c(\Gamma/Z) \cdot c(Z)$, where $Z = C_\Gamma(E)$ is the centralizer of E in Γ, $c(\Gamma/Z)$ is the number of complements of E in Γ/Z, and $c(Z)$ is the number of complements of E in Z. Next, it is shown that $c(\Gamma/Z) = |E|^\zeta$, and $c(Z) = |\mathrm{End}_\Gamma(E)|^{\alpha-1}$. Finally, it is noted that $|\mathrm{End}_\Gamma(E)| = q^\kappa$, for some $\kappa \geq 0$.

For related results, see [2, (2.10)] and [7, Theorem 2].

12

4.3 A recursion formula

Now let G be a finitely presented group.

Lemma 4.4 *Suppose* $\Gamma = E \times_{\sigma, \chi} B$ *is an extension of a finite group* B *by an elementary abelian* q-*group* E *which is a minimal normal subgroup of* Γ. *Then:*

$$|\mathrm{Epi}(G, \Gamma)| = \sum_{\rho \in \mathrm{Epi}(G, B)} \left(\epsilon_\chi(\rho) q^{d(\sigma \rho)} - c \right), \qquad (4.2)$$

where $c = c(\Gamma) = c_\chi |Z_\sigma^1(B, E)|$ *is the number of complements of* E *in* Γ *($c_\chi = 1$ if the extension splits, in which case $\epsilon_\chi(\rho) = 1$, and $c_\chi = 0$ otherwise).*

PROOF. Fix an epimorphism $\rho \colon G \to B$. Then ρ has $\left| Z_{\sigma \rho, \chi}^1(G, E) \right| = \epsilon_\chi(\rho) \cdot q^{d(\sigma \rho)}$ lifts to Γ. Let $\lambda \colon G \to \Gamma$ be such a lift, and let $U = \mathrm{Im}\,\lambda$. Then U is an extension of B by $K = U \cap E$ (a subgroup of E). By minimality, B acts irreducibly on E, and so either $K = E$, in which case $U = \Gamma$ (and so λ is surjective), or $K = 1$, in which case U is a complement of E. Therefore ρ contributes $\epsilon_\chi(\rho) q^{d(\sigma \rho)} - c$ to $|\mathrm{Epi}(G, \Gamma)|$. $\square$

We now have:

$$
\begin{aligned}
q^{d(\sigma \rho)} &= \left| Z_{\sigma \rho}^1(G, E) \right| \\
&= \left| B_{\sigma \rho}^1(G, E) \right| \cdot \left| H_{\sigma \rho}^1(G, E) \right| \\
&= |E|^\zeta \cdot q^{\dim_{\mathbb{Z}_q} H_{\sigma \rho}^1(G, E)}.
\end{aligned}
\qquad (4.3)
$$

Combining Lemma 4.4 with Theorem 4.2 and formula (4.3), we obtain the following.

Theorem 4.5 *Let* G *be a finitely presented group, and let* $\Gamma = E \times_{\sigma, \chi} B$ *be an extension of a finite, solvable group* B *by an elementary abelian* q-*group* E *which is a minimal normal subgroup of* Γ. *Then:*

$$|\mathrm{Epi}(G, \Gamma)| = |E|^\zeta \sum_{\rho \in \mathrm{Epi}(G, B)} \left(\epsilon_\chi(\rho) q^{\dim_{\mathbb{Z}_q} H_{\sigma \rho}^1(G, E)} - c_\chi q^{\kappa(\alpha - 1)} \right).$$

This Theorem allows us to compute recursively $|\mathrm{Aut}(\Gamma)| = |\mathrm{Epi}(\Gamma, \Gamma)|$, for any finite solvable group Γ.

Corollary 4.6 *Let* $\Gamma = E \times_{\sigma, \chi} B$ *be an extension of a finite, solvable group* B *by an elementary abelian* q-*group* E *which is a minimal normal subgroup of*

Γ. *Then:*

$$|\mathrm{Aut}(\Gamma)| = |E|^{\zeta} \sum_{\rho \in \mathrm{Epi}(\Gamma, B)} \left(\epsilon_\chi(\rho) q^{\dim_{\mathbb{Z}_q} H^1_{\sigma\rho}(\Gamma, E)} - c_\chi q^{\kappa(\alpha-1)} \right).$$

Combining the two results above gives a recursion formula for the Hall invariant $\delta_\Gamma(G)$, for any finite solvable group Γ.

4.7 Lifting through the chief series

We now describe an explicit procedure for constructing the set $\mathrm{Epi}(G, \Gamma)$, and counting its elements. Start with a chief series

$$\Gamma = \Gamma_0 > \Gamma_1 > \cdots > \Gamma_\nu > \Gamma_{\nu+1} = 1. \tag{4.4}$$

Write $E_i = \Gamma_i / \Gamma_{i+1} = \mathbb{Z}_{q_i}^{\oplus s_i}$ and $B_i = \Gamma / \Gamma_i$, for $0 \leq i \leq \nu$. Let $\chi_i \colon B_i \times B_i \to E_i$ be a classifying 2-cocycle for the extension

$$1 \longrightarrow E_i \longrightarrow B_{i+1} \longrightarrow B_i \longrightarrow 1, \tag{4.5}$$

with monodromy $\sigma_i \colon B_i \to \mathrm{Aut}(E_i) = \mathrm{GL}(s_i, q_i)$. Finally, let $c_i = c(B_{i+1})$ be the number of complements of E_i in B_{i+1}, let α_i be the number of chief factors of B_{i+1} isomorphic to E_i as B_{i+1}-modules, and set $q_i^{\kappa_i} = \left| \mathrm{End}_{B_{i+1}}(E_i) \right|$.

Now let G be a finitely presented group. Start with the trivial epimorphism $\rho_0 \colon G \to B_0 = 1$. Then $\mathrm{Epi}(G, B_1)$ consists of $q_0^{\beta_0} - 1$ elements, where $\beta_0 = \dim_{\mathbb{Z}_{q_0}} H^1(G; E_0)$.

For each such element $\rho_1 \colon G \twoheadrightarrow B_1$, we must decide whether there is a lift $\rho_2 \colon G \twoheadrightarrow B_2$. Applying Theorem 4.5 to the extension $B_2 = E_1 \times_{\sigma_1, \chi_1} B_1$, we find there are $|E_1|^{\zeta_1} \sum_{\rho_1 \in \mathrm{Epi}(G, B_1)} \left(\epsilon_{\chi_1}(\rho_1) q_1^{\beta_1} - c_{\chi_1} q_1^{\kappa_1(\alpha_1 - 1)} \right)$ such lifts, where

$\beta_1 = \dim_{\mathbb{Z}_{q_1}} H^1_{\sigma_1 \rho_1}(G, E_1).$

$$(4.6)$$
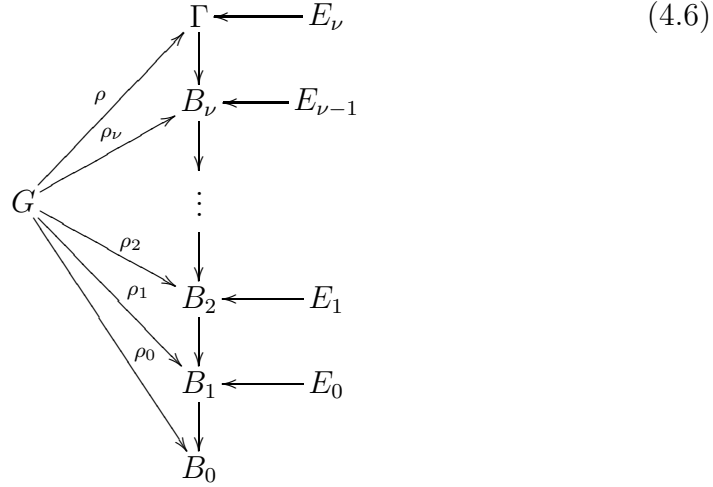
Continuing in the manner illustrated in diagram (4.6), we obtain the following formula.

Corollary 4.8 *With notation as above, the number of epimorphisms $\rho\colon G \twoheadrightarrow \Gamma$ is given by*

$$|\text{Epi}(G,\Gamma)| = \sum_{\rho_1 \in \text{Epi}_{\rho_0}(G,B_1)} \cdots \sum_{\rho_\nu \in \text{Epi}_{\rho_{\nu-1}}(G,B_\nu)} |E_\nu|^{\zeta_\nu}\left(\epsilon_{\chi_\nu}(\rho_\nu)q_\nu^{\beta_\nu} - c_{\chi_\nu}q_\nu^{\kappa_\nu(\alpha_\nu-1)}\right),$$

where $B_{\nu+1} = E_\nu \times_{\sigma_\nu,\chi_\nu} B_\nu$, $\beta_\nu = \dim_{\mathbb{Z}_{q_\nu}} H^1_{\sigma_\nu\rho_\nu}(G, E_\nu)$, α_ν is the number of complemented chief factors in $B_{\nu+1}$, isomorphic to E_ν as $B_{\nu+1}$-modules, and $\text{Epi}_{\rho_i}(G, B_{i+1})$ is the set of epimorphisms lifting $\rho_i\colon G \twoheadrightarrow B_i$.

When G is the free group of rank n, Theorem 4.5 (or Corollary 4.8) recovers the classical Gaschütz formula.

Corollary 4.9 ([11], Satz 4) *The Eulerian function of a finite solvable group, $\phi(\Gamma, n) = |\text{Epi}(F_n, \Gamma)|$, is given by*

$$\phi(\Gamma, n) = \prod_{i=1}^{h} \left[q_i^{s_i v_i n}\left(q_i^{s_i n} - q_i^{s_i \zeta_i}\right)\left(q_i^{s_i n} - q_i^{s_i \zeta_i + \kappa_i}\right) \cdots \left(q_i^{s_i n} - q_i^{s_i \zeta_i + (u_i-1)\kappa_i}\right)\right],$$

where $V_1, V_2, \ldots, V_h$ are the distinct Γ-module isomorphism types of the chief factors, $q_i^{s_i} = |V_i|$, $\zeta_i = 0$ or 1 according as Γ acts trivially on V_i or not, $q_i^{\kappa_i}$ is the number of Γ-endomorphisms of V_i, and finally, u_i is the numbers of factors of type V_i which are complemented in Γ, and v_i is the number of other factors of type V_i.

PROOF. Let E be a minimal normal subgroup of Γ, and set $B = \Gamma/E$. Let V_i

15

be the Γ-isomorphism type of E. Applying Theorem 4.5 we find an expression of the form:

$$|\mathrm{Epi}(F_n, \Gamma)| = |\mathrm{Epi}(F_n, B)| \cdot |E|^{\zeta_i} \left(q_i^{\beta_i} - c_{\chi_i} q_i^{\kappa_i(\alpha_i - 1)} \right),$$

where $\beta_i = \dim_{\mathbb{Z}_{q_i}} H^1(F_n, E) = s_i(n - \zeta_i)$. If E is not complemented, then $c_{\chi_i} = 0$, and the second factor reduces to $q_i^{s_i n}$; otherwise, the second factor reduces to $q_i^{s_i n} - q_i^{s_i \zeta_i + (u_i - 1)\kappa_i}$.

Now repeat the procedure, with Γ replaced by B, and continue in this fashion till the trivial group is reached. $\square$

5   Dihedral groups

We now study in more detail epimorphisms to the dihedral group of order $2m$. This group is a split extension $D_{2m} = \mathbb{Z}_m \rtimes_\sigma \mathbb{Z}_2$, with monodromy $\sigma(b) = b^{-1}$:

$$D_{2m} = \langle a, b \mid a^m = b^2 = 1,\ bab = a^{-1} \rangle.$$

Let $m = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ be the prime decomposition of m. A chief series for D_{2m} is

$$D_{2m} = \Gamma_0 > \Gamma_{1,1} > \cdots > \Gamma_{1,\alpha_1} > \cdots > \Gamma_{r,1} > \cdots > \Gamma_{r,\alpha_r} > 1,$$

with terms $\Gamma_{i,j} = \mathbb{Z}_{m/(q_1^{\alpha_1} \cdots q_{i-1}^{\alpha_{i-1}} q_i^{j-1})}$. The chief factors are $E_0 = \mathbb{Z}_2$ and $E_{i,j} = \mathbb{Z}_{q_i}$. The lifting process goes through the extensions $B_1 = \mathbb{Z}_2$ and $B_{i,j} = D_{2q_1^{\alpha_1} \cdots q_{i-1}^{\alpha_{i-1}} q_i^{j-1}}$, for $1 \le i \le r$, $1 \le j \le \alpha_i$. Of these extensions, only the ones where a prime q_i appears for the first time are split, while the others are non-split. Indeed, all the extensions are of the form $D_{2ql} = \mathbb{Z}_q \rtimes_{\sigma, \chi} D_{2l}$, with $\chi(a^u b^v, a^s b^t) = k$, where $u + s \cdot (-1)^v = l \cdot k + r \pmod{ql}$, and $0 \le r < l$.

As before, let G be a finitely presented group. Applying Lemma 4.4, we obtain the following recursion formula for the number of epimorphisms from G to a dihedral group:

$$|\mathrm{Epi}(G, D_{2ql})| = \begin{cases} \sum_{\rho \in \mathrm{Epi}(G, D_{2l})} \left(q^{d(\sigma\rho)} - q \right) & \text{if } q \nmid l, \\ \sum_{\rho \in \mathrm{Epi}(G, D_{2l})} \epsilon_\chi(\rho) q^{d(\sigma\rho)} & \text{if } q \mid l. \end{cases} \tag{5.1}$$

Example 5.1 For the free group $G = F_n$, we find:

$$|\mathrm{Epi}(F_n, D_{2m})| = (2^n - 1)m^n \cdot \prod_{i=1}^{r} (1 - q_i^{1-n}), \tag{5.2}$$

where $q_1, \ldots, q_r$ are the prime factors of m (and the empty product is 1). This recovers a computation of Kwak, Chun, and Lee, see [20, Lemma 4.1].

16

Example 5.2 Let $\Pi_g = \langle x_1, \ldots, x_g, y_1, \ldots, y_g \mid [x_1, y_1] \cdots [x_g, y_g] = 1 \rangle$ and $\Pi_g^* = \langle x_1, \ldots, x_g \mid x_1^2 \cdots x_g^2 = 1 \rangle$ be the fundamental groups of orientable (respectively, non-orientable) surfaces of genus g. Let $q_1, \ldots, q_r$ be the odd prime factors of m, and put $e = m/2 \pmod 2$ if m is even. Then, according to whether m is odd or even,

$$
|\mathrm{Epi}(\Pi_g, D_{2m})| = \begin{cases} m^{2g-1}(2^{2g} - 1) \displaystyle\prod_{i=1}^{r} \left(1 - q_i^{2-2g}\right), \\[2ex] m^{2g-1}(2^{2g} - 1)(2^e - 2^{2-2g}) \displaystyle\prod_{i=1}^{r} \left(1 - q_i^{2-2g}\right), \end{cases} \tag{5.3}
$$

$$
\left|\mathrm{Epi}(\Pi_g^*, D_{2m})\right| = \begin{cases} m^{g-1}\left[(2^g - 2) \displaystyle\prod_{i=1}^{r} \left(1 - q_i^{2-g}\right) + \prod_{i=1}^{r} \left(q_i - q_i^{2-g}\right)\right], \\[2ex] m^{g-1}(2^e - 2^{2-g})\left[(2^g - 2) \displaystyle\prod_{i=1}^{r} \left(1 - q_i^{2-g}\right) + \prod_{i=1}^{r} \left(q_i - q_i^{2-g}\right)\right]. \end{cases}
$$

In [19], Kwak and Lee obtained related formulas, counting the number of regular, D_{2p} branched covers (p prime) of a closed surface.

Example 5.3 An interesting family of examples is provided by the Baumslag-Solitar one-relator groups $\mathrm{BS}(m, n) = \langle x, y \mid xy^m x^{-1} y^{-n} \rangle$. As an illustration of our techniques, we now compute the number of epimorphisms from $G = \mathrm{BS}(m, n)$ to D_8.

The dihedral group D_8 is a central extension of $\mathbb{Z}_2^{\oplus 2}$ by $\mathbb{Z}_2$, with 2-cocycle $\chi \colon \mathbb{Z}_2^{\oplus 2} \times \mathbb{Z}_2^{\oplus 2} \to \mathbb{Z}_2$ assuming non-zero values only on the pairs (a, a), (b, a), (a, ab), and (b, ab). An epimorphism $G \twoheadrightarrow D_8$ induces by abelianization an epimorphism $\mathbb{Z} \oplus \mathbb{Z}_{|n-m|} \twoheadrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$; this can happen only if m and n have the same parity.

So assume $m \equiv n \pmod 2$. Then there are precisely 6 epimorphisms from G to $\mathbb{Z}_2^{\oplus 2}$; let $\rho \colon G \twoheadrightarrow \mathbb{Z}_2^{\oplus 2}$ be one of those. A computation shows that $J_G^\rho = 0$. By Theorem 3.4, ρ lifts to D_8, i.e., $\epsilon_\chi(\rho) = 1$, if and only if

$$
\sum_{k=1}^{m} \chi\left(uv^{k-1}, v\right) - \chi(u, u) + \chi(uv^m, u) + \sum_{l=1}^{n} \left(-\chi(v, v) + \chi(uv^m uv^{l-1}, v)\right) = 0.
$$

where $u = \rho(x)$ and $v = \rho(y)$, in which case there are precisely 4 lifts to D_8. This equation simplifies to

$$
\tfrac{m}{2}\chi(u, v) + \tfrac{m}{2}\chi(uv, v) + \tfrac{n}{2}\chi(v, v) = 0, \quad \text{or}
$$
$$
\tfrac{m+1}{2}\chi(u, v) + \tfrac{m-1}{2}\chi(uv, v) + \tfrac{n-1}{2}\chi(v, v) + \chi(uv, u) - \chi(u, u) = 0,
$$

according to whether m is even or odd. We find that $|\{\rho \mid \epsilon_\chi(\rho) = 1\}| = 6, 4, 2,$ or 0, according to whether $(m, \frac{n-m}{2}) \equiv (0, 0), (0, 1), (1, 1),$ or $(1, 0)$ mod-

ulo 2, respectively. Using the fact that $\text{Aut}(D_8) = D_8$, we obtain:

$$
\delta_{D_8}(\text{BS}(m,n)) = \begin{cases} 3 & \text{if } m \text{ even and } n - m \equiv 0 \ (\text{mod } 4), \\ 2 & \text{if } m \text{ even and } n - m \equiv 2 \ (\text{mod } 4), \\ 1 & \text{if } m \text{ odd} \ \text{ and } n - m \equiv 2 \ (\text{mod } 4), \\ 0 & \text{otherwise.} \end{cases} \tag{5.4}
$$

6 Binary dihedral groups

The binary dihedral group of order $4m$ is a central extension $D_{4m}^* = \mathbb{Z}_2 \times_\chi D_{2m}$, with presentation

$$
D_{4m}^* = \langle a, b \mid a^{2m} = 1, \ a^m = b^2, \ bab^{-1} = a^{-1} \rangle.
$$

In particular, $D_4^* = \mathbb{Z}_4$, $D_8^* = Q_8$, the quaternion group, and $D_{4 \cdot 2^{m-2}}^* = Q_{2^m}$, the generalized quaternion group. Write $m = q_0^{\alpha_0} q_1^{\alpha_1} \cdots q_r^{\alpha_r}$, with $q_0 = 2$. A chief series is then:

$$
D_{4m}^* = \Gamma_0 > \Gamma_{0,0} > \Gamma_{0,1} > \cdots > \Gamma_{0,\alpha_0} > \cdots > \Gamma_{r,1} > \cdots > \Gamma_{r,\alpha_r} > 1,
$$

with terms $\Gamma_{0,0} = \mathbb{Z}_{2m}$, $\Gamma_{i,j} = \mathbb{Z}_{m/(q_0^{\alpha_0} \cdots q_{i-1}^{\alpha_{i-1}} q_i^{j-1})}$ and factors $E_{0,0} = \mathbb{Z}_2$, $E_{i,j} = \mathbb{Z}_{q_i}$, where $0 \leq i \leq r$, $1 \leq j \leq \alpha_i$. The lifting process goes through the extensions $B_0 = \mathbb{Z}_2$, $B_{0,j} = D_{2^{j+2}}$, and $B_{i,j} = D_{4q_0^{\alpha_0} \cdots q_{i-1}^{\alpha_{i-1}} q_i^{j-1}}^*$. Here only the extensions where a prime q_i appears for the first time are split, the rest are non-split, except when m is even, in which case the prime $q_0 = 2$ produces a split extension the first two times it appears.

Indeed, there are three types of extensions that occur:

- $D_{2ql}^* = \mathbb{Z}_q \times_{\sigma,\chi} D_{2l}^*$, with q an odd prime, in which case the computation of χ goes essentially as in the dihedral case.
- $D_{2^{r+1}} = \mathbb{Z}_2 \times_\chi D_{2^r}$, for which χ was computed before.
- $Q_{2^{r+1}} = \mathbb{Z}_2 \times_\chi D_{2^r}$, in which case $\chi(a^u b^v, a^s b^t) = k + l$, where $u + s \cdot (-1)^v \equiv k \cdot 2^{r-1} + n \ (\text{mod } 2^r)$ with $0 \leq n < 2^{r-1}$, and $l = 1$ if $v = t = 1$ and $l = 0$ otherwise.

Applying Lemma 4.4, we obtain the following recursion formulas:

$$\left|\mathrm{Epi}(G, D_{2ql}^*)\right| = \begin{cases} \displaystyle\sum_{\rho\in\mathrm{Epi}(G,D_{2l}^*)} \left(q^{d(\sigma\rho)} - q\right) & \text{if } q \nmid l, \\ \displaystyle\sum_{\rho\in\mathrm{Epi}(G,D_{2l}^*)} \epsilon_\chi(\rho)q^{d(\sigma\rho)} & \text{if } q \mid l, \end{cases} \tag{6.1}$$

$$|\mathrm{Epi}(G, Q_{2^{r+1}})| = \sum_{\rho\in\mathrm{Epi}(G,D_{2^r})} \epsilon_\chi(\rho)q^{d(\rho)}. \tag{6.2}$$

Example 6.1 For the free group $G = F_n$, we find:

$$|\mathrm{Epi}(F_n, D_{4m}^*)| = (4^n - 2^n)m^n \cdot \prod_{i=0}^{r}(1 - q_i^{1-n}). \tag{6.3}$$

Example 6.2 Let us compute the number of epimorphisms from the Baumslag-Solitar groups to the quaternion group. Notice that $Q_8 = \mathbb{Z}_2 \times_\chi \mathbb{Z}_2^{\oplus 2}$, with 2-cocycle χ vanishing only on the pairs (a, b), (b, ab), and (ab, a). Let $\rho\colon \mathrm{BS}(m, n) \twoheadrightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ be an epimorphism. Then necessarily m and n have the same parity. Moreover, ρ lifts to Q_8 if and only if

$$\sum_{k=1}^{m}\chi(uv^{k-1}, v) - \chi(u, u) + \chi(uv^m, u)+$$

$$\sum_{l=1}^{n}\left(-\chi(v, v) + \chi(uv^m uv^{l-1}, v)\right) = 0,$$

where $u = \rho(x)$ and $v = \rho(y)$, in which case ρ has 4 lifts. The above condition is equivalent to $m + n \equiv 0 \pmod 4$. Using the fact that $\mathrm{Aut}(Q_8) = S_4$, we conclude:

$$\delta_{Q_8}(\mathrm{BS}(m, n)) = \begin{cases} 1 & \text{if } n - m \text{ is even and } m + n \equiv 0 \pmod 4, \\ 0 & \text{otherwise.} \end{cases} \tag{6.4}$$

7 Finite quotients of derived length 3

We now consider epimorphisms of a finitely presented group G onto finite groups which are not metabelian. A nice class of groups of derived length 3 are the split extensions $\Gamma = \mathbb{Z}_q^2 \rtimes_\sigma D_{2p}$, where p and q are distinct primes such that q has order 2 (mod p). On generators b and c for D_{2p}, the monodromy $\sigma\colon D_{2p} \to \mathrm{GL}(2, q)$ is given by $\sigma(b) = \left(\begin{smallmatrix} r & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $\sigma(c) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, for some r.

According to Theorem 4.5, we have:

$$|\mathrm{Epi}(G, \Gamma)| = q^2 \sum_{\rho\in\mathrm{Epi}(G,D_{2p})} \left(q^{\beta(\rho)} - 1\right), \tag{7.1}$$

19

where $\beta(\rho) = \dim_{\mathbb{Z}_q} H^1_{\sigma\rho}(G; \mathbb{Z}_q^{\oplus 2})$.

In particular, the symmetric group on four letters is a split extension $S_4 = \mathbb{Z}_2^{\oplus 2} \rtimes_\sigma S_3$, with monodromy $\sigma\colon S_3 = \mathrm{SL}(2,2) \to \mathrm{Aut}(\mathbb{Z}_2^{\oplus 2}) = \mathrm{GL}(2,2)$ the natural inclusion, given by $\sigma(b) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\sigma(c) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. We then have: $|\mathrm{Epi}(G, S_4)| = 4\sum_{\rho \in \mathrm{Epi}(G,S_3)} \left(2^{\beta(\rho)} - 1\right)$, where $\beta(\rho) = \dim_{\mathbb{Z}_2} H^1_{\sigma\rho}(G; \mathbb{Z}_2^{\oplus 2})$. Since $\mathrm{Aut}(S_4) = S_4$, we find:

$$\delta_{S_4}(G) = \tfrac{1}{6} \sum_{\rho \in \mathrm{Epi}(G,S_3)} \left(2^{\beta(\rho)} - 1\right). \tag{7.2}$$

Example 7.1 Consider $G = F_n$. Recall that $|\mathrm{Epi}(F_n, S_3)| = (2^n - 1)(3^n - 3)$. If $\rho\colon F_n \twoheadrightarrow S_3$, then $H^1_{\sigma\rho}(F_n; \mathbb{Z}_2^{\oplus 2}) = \mathbb{Z}_2^{\oplus 2n-2}$. Hence,

$$|\mathrm{Epi}(F_n, S_4)| = (2^n - 1)(3^n - 3)(4^n - 4). \tag{7.3}$$

Example 7.2 Let $G = \langle x, y \mid yxy^{-1} = x^{-1} \rangle$ be the Klein bottle group. There is then an obvious epimorphism $\rho\colon G \twoheadrightarrow S_3$; in fact, $\delta_{S_3}(G) = 1$. But this epimorphism does not lift to S_4. Indeed, $J_G = (\, y + x^{-1} \quad 1 - x^{-1} \,)$, and thus $J_G^{\sigma\rho} = \left(\begin{smallmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{smallmatrix}\right)$. Hence, $H^1_{\sigma\rho}(G, \mathbb{Z}_2^{\oplus 2}) = 0$, and so $\delta_{S_4}(G) = 0$.

Example 7.3 We now show that the Baumslag parafree groups, $P(m, n) = \langle x, y, z \mid xz^m x z^{-m} x^{-1} z^n y z^{-n} y^{-1} \rangle$, fall into at least two distinct isomorphism classes, each containing infinitely many members. We do this by counting epimorphisms to S_4.

Let us start by computing the Fox Jacobian of $G = P(m, n)$:

$$J_G = \left(1 + xz^m - [y, z^n] \quad yz^n y^{-1} - 1 \quad x(1 - z^m xz^{-m})s_m + ([y, z^n] - y)s_n\right),$$

where $s_k = 1 + z + \cdots + z^{k-1}$. The abelianization $\mathrm{ab}\colon G \to G/G' = \mathbb{Z}^2 = \langle t_1, t_2 \rangle$ sends $x \mapsto 1$, $y \mapsto t_1$, $z \mapsto t_2$. Thus,

$$J_G^{\mathrm{ab}} = \left(t_2^m \quad t_2^n - 1 \quad (1 - t_1)(1 + t_2 + \cdots + t_2^{n-1})\right).$$

Clearly, $|\mathrm{Epi}(G, \mathbb{Z}_2)| = 3$. Since the first entry in J_G^{ab} is never zero, each epimorphism $G \twoheadrightarrow \mathbb{Z}_2$ lifts to 6 different epimorphisms to S_3. Writing the typical element of $S_3 = \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ as $b^\beta c^\gamma$, we see that the 18 epimorphisms $\rho\colon G \twoheadrightarrow S_3$ divide into 3 families:

- $x \to b^\beta, y \to b^{\beta_1} c, z \to b^{\beta_2}$, where $\beta = n\beta_2 \neq 0$ and β_1 arbitrary,
- $x \to b^\beta, y \to b^{\beta_1}, z \to b^{\beta_2} c$, where $\beta = ((-1)^m - (-1)^{m+n})\beta_1 \neq 0$ and β_2 arbitrary,
- $x \to b^\beta, y \to b^{\beta_1} c, z \to b^{\beta_2}$, where $\beta = ((-1)^m - (-1)^{m+n})(\beta_1 - \beta_2) \neq 0$.

20

Each ρ in the first family contributes $4(2^2 - 1)$ to $|\mathrm{Epi}(G, S_4)|$, as $J^{\sigma\rho}$ has corank 4, while the other ρ's contribute either $4(2^3 - 1)$ or $4(2^2 - 1)$, according as $J^{\sigma\rho}$ has corank 5 or 4 (depending on whether $m - n \equiv 2 \pmod 4$ or not). Therefore

$$\delta_{S_4}(P(m,n)) = \begin{cases} \frac{6 \cdot 4(2^2-1)+12 \cdot 4(2^3-1)}{24} = 17 & \text{if } m \text{ odd}, m - n \equiv 2 \pmod 4, \\ \frac{18 \cdot 4(2^2-1)}{24} = 9 & \text{otherwise.} \end{cases}$$

$$(7.4)$$

It would be interesting to see whether solvable Hall invariants completely classify the Baumslag parafree groups, and, more generally, the parafree groups considered by Strebel in [30].

Example 7.4 Let L be the 2-component link from [16, p. 72], and G the fundamental group of its complement, with presentation

$$G = \left\langle x_1, x_2, x_3, x_4 \; \middle| \; \begin{array}{l} x_1^{x_4^{-1}} (x_4 x_1)^{x_2^{-1} x_1 x_2}, \quad (x_3^{-1} x_1 x_4)^{x_2^{-1} x_1^{-1} x_2} (x_1 x_4)^{x_3} \\ [x_1^{-1} x_4^{-1} x_3 x_1 x_4 x_3^{-2} x_4, x_2] \end{array} \right\rangle,$$

where $x^y = y^{-1} x y$. Let G_ω be the intersection of the lower central series of G. As noted by Hillman, $G = G_\omega \rtimes P(-1, 1)$. In particular, L is not a homology boundary link. Moreover, $G/G'' \cong F_2/F_2''$, yet $G \not\cong F_2$.

Notice that $|\mathrm{Epi}(G, \Gamma)| = |\mathrm{Epi}(F_2, \Gamma)|$, for any finite metabelian group Γ. In particular, $\delta_{S_3}(G) = 3$. On the other hand, we can distinguish G from both F_2 and $P(-1, 1)$ by counting representations onto S_4:

$$\delta_{S_4}(G) = 2 \cdot (2^4 - 1) + (2^2 - 1) = 33.$$

8   The lattice of subgroups

Let Γ be a finite group. Let $L(\Gamma)$ be the lattice of subgroups of Γ, ordered by inclusion. The *Möbius function*, $\mu \colon L(\Gamma) \times L(\Gamma) \to \mathbb{Z}$, is defined inductively by $\mu(H, H) = 1$, and $\sum_{H \leq S \leq K} \mu(H, S) = 0$, for any subgroup $K \leq \Gamma$. For simplicity, write $\mu(H) := \mu(H, \Gamma)$.

In [18], Kratzer and Thévenaz give a formula for the Möbius function of a solvable group, in terms of a chief series.

Theorem 8.1 ([18]) *Suppose Γ is solvable, and let $\Gamma = \Gamma_0 > \cdots > \Gamma_\nu > 1$ be a chief series. If $H \leq \Gamma$, let $H_i = \Gamma_i H$, and consider the sequence $H = H_r < \cdots < H_0 = \Gamma$, where one keeps only distinct terms H_i. Let h_i be the number*

of complements of H_i in $L(\Gamma)$ which contain H_{i+1}. Then

$$\mu(H) = (-1)^r h_1 \cdots h_{r-1}.$$

In the particular case when Γ is nilpotent, this recovers a classical result of Weisner: $\mu(H) = 0$, unless $H \triangleleft \Gamma$ and $\Gamma/H \cong \bigoplus_{i=1}^r \mathbb{Z}_{q_i}^{\oplus s_i}$, in which case $\mu(H) = \prod_{i=1}^r (-1)^{s_i} q_i^{s_i(s_i-1)/2}$.

Now let G be a finitely generated group. Then, as noted by P. Hall [15],

$$|\mathrm{Hom}(G, \Gamma)| = \sum_{H \leq \Gamma} |\mathrm{Epi}(G, H)|, \qquad (8.1)$$

or, by Möbius inversion:

$$|\mathrm{Epi}(G, \Gamma)| = \sum_{H \leq \Gamma} \mu(H) |\mathrm{Hom}(G, H)|. \qquad (8.2)$$

The *Eulerian function* of Γ is the sequence $\phi(\Gamma, n) = |\mathrm{Epi}(F_n, \Gamma)|$, counting ordered n-tuples generating Γ. By the Hall enumeration principle (8.2), the Eulerian function is determined by the Möbius function, as follows: $\phi(\Gamma, n) = \sum_{H \leq \Gamma} \mu(H) |H|^n$.

In conjunction with the results from Section 2, the Hall enumeration principle provides an alternate way to compute the number of epimorphisms from an arbitrary finitely presented group G to a finite solvable group Γ.

Example 8.2 The lattice of subgroups of the dihedral group D_{2m} consists of one subgroup of type $\mathbb{Z}_l$ and m/l subgroups of type D_{2l}, for each divisor l of m. The Möbius function is given by

$$\mu(\mathbb{Z}_l) = -\tfrac{m}{l}\mu(\tfrac{m}{l}), \qquad \mu(D_{2l}) = \mu(\tfrac{m}{l}).$$

Let $q_1, \dots, q_r$ be the prime divisors of m. By Proposition 3.2 and formula (3.8), we have:

$$
\begin{aligned}
|\mathrm{Epi}(G, D_{2m})| &= \sum_{l|m} \tfrac{1}{l}\mu(\tfrac{m}{l}) \left(|\mathrm{Hom}(G, D_{2l})| - |\mathrm{Hom}(G, \mathbb{Z}_l)|\right) \\
&= \sum_{l|m} \tfrac{1}{l}\mu(\tfrac{m}{l}) \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_2)} \left|Z^1_{\sigma\rho}(G, \mathbb{Z}_l)\right| \qquad (8.3) \\
&= \sum_{l|m} \tfrac{1}{l}\mu(\tfrac{m}{l}) \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_2)} \prod_{i=1}^r q_i^{d(\pi_{q_i}\sigma\rho)}.
\end{aligned}
$$

In particular, $|\mathrm{Epi}(F_n, D_{2m})| = (2^n - 1)\sum_{l|m}\tfrac{m}{l}\mu(\tfrac{m}{l})l^n$, which, after some manipulations, recovers formula (5.2).

22

9 Hall invariants and finite-index subgroups

Let G be a finitely generated group. For each positive integer k, let $a_k(G)$ be the number of index k subgroups of G. The behavior of the sequence $\{a_k(G)\}_{k \geq 1}$ (that is, the "subgroup growth" of G) has been the object of intense study ever since the foundational paper of M. Hall [14]; see the monograph by A. Lubotzky and D. Segal [25] for a comprehensive survey.

Let $h_k(G) = |\mathrm{Hom}(G, S_k)|$ and $t_k(G)$ be the number of homomorphisms (respectively, transitive homomorphisms) from G to the symmetric group S_k. It is readily seen that $a_k(G) = \frac{t_k(G)}{(k-1)!}$. The following recursion formula (due to M. Hall [14]) computes a_k in terms of $h_1, \ldots, h_k$, starting from $a_1 = h_1 = 1$:

$$a_k(G) = \frac{1}{(k-1)!} h_k(G) - \sum_{l=1}^{k-1} \frac{1}{(k-l)!} h_{k-l}(G) a_l(G). \tag{9.1}$$

In this context, it is also useful to consider the Γ-*Hall invariant* of G,

$$\delta_\Gamma(G) = |\mathrm{Epi}(G, \Gamma)| / |\mathrm{Aut}\,\Gamma|. \tag{9.2}$$

Since $\mathrm{Aut}\,\Gamma$ acts freely and transitively on $\mathrm{Epi}(G, \Gamma)$, the number $\delta_\Gamma(G)$ is an integer, which counts the homomorphic images of G that are isomorphic to Γ. Notice that $\delta_{\Gamma_1 \times \Gamma_2}(G) = \delta_{\Gamma_1}(G) \delta_{\Gamma_2}(G)$, provided Γ_1 and Γ_2 have coprime orders.

Formula (9.1), together with P. Hall's enumeration principle (8.1), expresses the numbers $a_k = a_k(G)$ in terms of Hall invariants. For low indices, we have: $a_1 = 1$, $a_2 = \delta_{\mathbb{Z}_2}$, $a_3 = \delta_{\mathbb{Z}_3} + 3\delta_{S_3}$, and

$$a_4 = \tfrac{1}{2}\delta_{\mathbb{Z}_2}(1 - \delta_{\mathbb{Z}_2}) + \delta_{\mathbb{Z}_4} + 4\delta_{\mathbb{Z}_2^{\oplus 2}} + 4\delta_{D_8} + 4\delta_{A_4} + 4\delta_{S_4}. \tag{9.3}$$

In general, the Hall invariants $\delta_\Gamma(G)$ contain more information about a group G than the numbers $a_k(G)$. For example, $a_k(\Pi_g) = a_k(\Pi_{2g}^*)$, for all $g \geq 1$ (see [25]), but clearly $\delta_{\mathbb{Z}_n}(\Pi_g) \neq \delta_{\mathbb{Z}_n}(\Pi_{2g}^*)$ for any odd $n > 1$.

When G is finitely presented, all the Hall invariants that appear in (9.3) can be expressed in terms of simple homological data. If Γ is abelian, this is done in Theorem 3.1 in [26]. Let us briefly review how this goes.

For a prime p, write the p-torsion part of $H_1(G, \mathbb{Z})$ as $\bigoplus_{i \geq 1} \mathbb{Z}_{p^i}^{\oplus \alpha_i}$. Set $n = \mathrm{rank}\, H_1(G, \mathbb{Z})$, $\alpha = \sum i\alpha_i$, and $\beta = \sum \alpha_i$. For a positive integer s, write

Γ	$\delta_\Gamma(G)$
$S_3 = \mathbb{Z}_3 \rtimes_\sigma \mathbb{Z}_2$	$\frac{1}{2} \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_2)} (3^{\dim_{\mathbb{Z}_3} H^1_{\sigma\rho}(G,\mathbb{Z}_3)} - 1)$
$D_8 = \mathbb{Z}_2 \rtimes_\chi \mathbb{Z}_2^{\oplus 2}$	$\frac{1}{8} \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_2^{\oplus 2})} \epsilon_\chi(\rho) 2^{\dim_{\mathbb{Z}_2} H^1_\rho(G,\mathbb{Z}_2)}$
$Q_8 = \mathbb{Z}_2 \times_\chi \mathbb{Z}_2^{\oplus 2}$	$\frac{1}{24} \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_2^{\oplus 2})} \epsilon_\chi(\rho) 2^{\dim_{\mathbb{Z}_2} H^1_\rho(G,\mathbb{Z}_2)}$
$D_{12} = \mathbb{Z}_3 \rtimes_\sigma \mathbb{Z}_2^{\oplus 2}$	$\frac{1}{4} \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_2^{\oplus 2})} \left(3^{\dim_{\mathbb{Z}_3} H^1_{\sigma\rho}(G,\mathbb{Z}_3)} - 1\right)$
$D_{12}^* = \mathbb{Z}_3 \rtimes_\sigma \mathbb{Z}_4$	$\frac{1}{4} \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_4)} (3^{\dim_{\mathbb{Z}_3} H^1_{\sigma\rho}(G,\mathbb{Z}_3)} - 1)$
$A_4 = \mathbb{Z}_2^{\oplus 2} \rtimes_\sigma \mathbb{Z}_3$	$\frac{1}{6} \sum_{\rho \in \mathrm{Epi}(G,\mathbb{Z}_3)} (2^{\dim_{\mathbb{Z}_2} H^1_{\sigma\rho}(G,\mathbb{Z}_2^{\oplus 2})} - 1)$

Table 1
Hall invariants for non-abelian groups of order at most 12.

$\alpha[s] = \sum_{i=1}^{s-1} i\alpha_i$. We then have:

$$\delta_{\mathbb{Z}_{p^s}}(G) = \frac{p^{sn+\alpha} - p^{(s-1)n+\alpha[s]}}{p^s - p^{s-1}},$$

$$\delta_{\mathbb{Z}_p^{\oplus s}}(G) = \prod_{i=0}^{s-1} \frac{p^{n+\beta} - p^i}{p^s - p^i}, \tag{9.4}$$

$$\delta_{\mathbb{Z}_p \oplus \mathbb{Z}_{p^s}}(G) = \frac{(p^{sn+\alpha} - p^{(s-1)n+\alpha[s]})(p^{n+\beta} - p)}{p^{s+1}(p-1)^2}.$$

These formulas, together with the multiplicativity property of δ determine the Γ-invariants of G for Γ abelian of order at most 31, while higher orders are treated similarly.

If Γ is non-abelian, of order at most 12, the answer is given in Table 1. Plugging these answers, together with the ones from (7.2) and (9.4) into formula (9.3) gives an expression for $a_4(G)$ solely in terms of cohomological invariants for G.

Now let $a_k^\triangleleft(G)$ be the number of index k, normal subgroups of G. Clearly,

$$a_k^\triangleleft(G) = \sum_{|\Gamma|=k} \delta_\Gamma(G). \tag{9.5}$$

In [26], we used this formula to compute $a_k^\triangleleft(G)$ in terms of homological data, provided k has at most two factors. Our approach worked for all $k \leq 15$, except for $k = 8$ and $k = 12$. To compute $a_8^\triangleleft$, we also needed to know δ_{D_8} and δ_{Q_8}; for $a_{12}^\triangleleft$, we also needed $\delta_{D_{12}}$ and $\delta_{D_{12}^*}$. The formulas in Table 1 complete the computation of $a_k^\triangleleft(G)$, for $k \leq 15$.

10 Finite quotients of braid groups

We conclude with a discussion of Artin's braid groups, viewed through the prism of their finite quotients and their finite-index subgroups. In addition to our own results, we use in crucial fashion results of Artin [1], Gorin and Lin [13], and Lin [22], [23], [24].

10.1 Braid groups

The braid group on $n \geq 3$ strings has presentation

$$B_n = \langle x, y \mid y^n (yx)^{1-n}, \ [y^i x y^{-i}, x], \ 2 \leq i \leq n/2 \rangle.$$

Let B'_n be the commutator subgroup. Clearly, $B_n/B'_n = \mathbb{Z}$, generated by x, and so we have a split extension, $B_n = B'_n \rtimes_\tau \mathbb{Z}$. It is also known that

$$B_3 = F_2 \rtimes_\tau \mathbb{Z} = \langle x, a, b \mid a^x = b, \ b^x = ba^{-1} \rangle,$$

$$B_4 = (F_2 \rtimes F_2) \rtimes_\tau \mathbb{Z} = \left\langle \begin{matrix} x, a, b \\ c, d \end{matrix} \middle| \begin{matrix} a^x = b, \ b^x = ba^{-1}, \ c^x = dc, \quad d^x = d, \\ c^a = d, \ c^b = d^{-1}c, \ d^a = dc^{-1}d^2, \ d^b = dc^{-1}d \end{matrix} \right\rangle.$$

Note that $B'_3/B''_3 = B'_4/B''_4 = \mathbb{Z}^2$. On the other hand, if $n \geq 5$, then B'_n is perfect, see Gorin and Lin [13].

Now suppose Γ is a finite group. If Γ is cyclic, then $\delta_\Gamma(B_n) = 1$. On the other hand, if Γ/Γ' is non-cyclic, then $\delta_\Gamma(B_n) = 0$.

If $n \geq 5$, and Γ is a finite quotient of B_n, then Γ' must be perfect. Hence, every finite solvable quotient of B_n must be cyclic, and so

$$\delta_\Gamma(B_n) = \begin{cases} 0 & \text{if } \Gamma \text{ is not cyclic,} \\ 1 & \text{if } \Gamma \text{ is cyclic,} \end{cases} \tag{10.1}$$

whenever Γ is a finite solvable group and $n \geq 5$. On the other hand, the groups B_3 and B_4 have plenty of non-abelian, finite solvable quotients, as we see next.

10.2 Solvable quotients of B_3 and B_4

Let G be one of the braid groups B_3 or B_4. From the presentations above it is apparent that the maximal metabelian quotient, G/G'', is isomorphic to $H = (\mathbb{Z} \oplus \mathbb{Z}) \rtimes_\tau \mathbb{Z}$. The monodromy action, $\tau = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix} \right)$, has order 6, and its characteristic polynomial is $t^2 - t + 1$.

Now let Γ be a finite, metabelian quotient of G. Then $\Gamma = \Gamma' \rtimes_{\bar\tau} \mathbb{Z}_k$, with Γ' a quotient of $\mathbb{Z}^2$. Write $\Gamma' = \mathbb{Z}_m \oplus \mathbb{Z}_l$. We can pick generators $z \in \mathbb{Z}_k$ and $u, v \in \Gamma'$ so that $\bar\tau(z) \in \mathrm{Aut}(\Gamma')$ is given by $\bar\tau(u) = v$ and $\bar\tau(v) = -u + v$. Hence, u and v have the same order, and so either $(m, l) = 1$ or $l = m$. Analyzing the various possibilities, we obtain the following Proposition.

Proposition 10.3 *Let Γ a finite, metabelian quotient of $G = B_3$ or B_4. Assume Γ is not cyclic. Then Γ is split metabelian, of type*

(1) $\Gamma = \mathbb{Z}_3 \rtimes \mathbb{Z}_k$ *with* $k \equiv \pm 2 \pmod 6$, *in which case* $\delta_\Gamma(G) = 1$;
(2) $\Gamma = \mathbb{Z}_r \rtimes \mathbb{Z}_k$ *with* $r > 3$ *and* $k \equiv 0 \pmod 6$, *in which case* $\delta_\Gamma(G) = 2$;
(3) $\Gamma = \mathbb{Z}_2^{\oplus 2} \rtimes \mathbb{Z}_k$ *with* $k \equiv 3 \pmod 6$, *in which case* $\delta_\Gamma(G) = 1$;
(4) $\Gamma = \mathbb{Z}_r^{\oplus 2} \rtimes \mathbb{Z}_k$ *with* $r > 3$ *and* $k \equiv 0 \pmod 6$, *in which case* $\delta_\Gamma(G) = 1$.

Now assume Γ is a finite, solvable, non-cyclic quotient of B_3 or B_4. If follows from the proof above that the maximal metabelian quotient, Γ/Γ'' has order divisible by 6. But Γ is an extension of Γ/Γ'', and so $|\Gamma|$ is also divisible by 6.

Finite solvable quotients of B_3 can have derived length greater than 2. For example, consider $S_4 = \mathbb{Z}_2^{\oplus 2} \rtimes S_3$. We know $|\mathrm{Epi}(B_3, S_3)| = 6$. If ρ is an epimorphism from B_3 to S_3, then $H^1_{\sigma\rho}(B_3; \mathbb{Z}_2^{\oplus 2}) = \mathbb{Z}_2$. Hence, $|\mathrm{Epi}(B_3, S_4)| = 4 \cdot 6 \cdot (2^1 - 1)$, and so $\delta_{S_4}(B_3) = 1$.

More generally, if $\Gamma_r = \mathbb{Z}_{2 \cdot 3^r} \rtimes_\chi A_4$ is the sequence of groups starting from $\Gamma_0 = S_4$, then $\delta_{\Gamma_r}(B_3) = 1$. On the other hand, if $\tilde\Gamma_r = \mathbb{Z}_{2 \cdot 3^r} \rtimes_{\tilde\chi} A_4$ is the sequence of groups starting from $\tilde\Gamma_0 = \mathrm{SL}(2, 3)$, then $\delta_{\tilde\Gamma_r}(B_3) = 2$.

Since B_4 surjects onto B_3, it inherits all the finite quotients of B_3. In general, though, B_4 has more epimorphisms onto a given finite quotient than B_3. The smallest solvable group for which this happens is S_4. Indeed, $H^1_{\sigma\rho}(B_4; \mathbb{Z}_2^{\oplus 2}) = \mathbb{Z}_2^{\oplus 2}$, for all $\rho \colon B_4 \twoheadrightarrow S_3$; thus, $|\mathrm{Epi}(B_4, S_4)| = 4 \cdot 6 \cdot (2^2 - 1)$, and so $\delta_{S_4}(B_4) = 3$, although $\delta_{S_4}(B_3) = 1$.

In view of all this evidence, we propose the following conjecture. Let Γ be a finite solvable group. Then

$$\delta_\Gamma(B_3) \le 2 \quad \text{and} \quad \delta_\Gamma(B_4) \le 3. \tag{10.2}$$

10.4 Finite-index subgroups of B_n

We conclude with a discussion of the subgroup growth of the braid groups B_n. Of course, $a_1(B_n) = a_2(B_n) = 1$. The values of $a_k(B_n)$ for $3 \le n \le 8$ and $3 \le k \le 16$ are listed in Table 2. The values not in bold were computed solely by machine. The values in bold can be justified, as follows.

	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}	a_{16}
B_3	4	9	6	22	43	49	130	266	287	786	1730	2199	5184	12193
B_4	4	17	6	34	43	81	148	266	287	938	1730	2199	5199	12449
B_5	1	1	6	7	1	1	1	26	1	19	1	1	36	17
B_6	1	1	1	13	1	1	1	11	1	25	1	1	31	1
B_7	1	1	1	1	8	1	1	1	1	1	1	22	1	1
B_8	1	1	1	1	1	9	1	1	1	1	1	1	1	25

Table 2

Number of low-index subgroups of B_n ($n \leq 8$)

(1) Using results from §10.2, we see that $a_3(B_3) = a_3(B_4) = 4$, and $a_3(B_n) = 1$, for $n > 4$. Furthermore, $a_4(B_3) = 9$, $a_4(B_4) = 17$, and $a_4(B_n) = 1$, for $n > 4$.

(2) Proposition 4.1 from Lin [24] give $t_k(B_3)$, for $4 \leq k \leq 7$, while Propositions 4.4 and 4.7 from [24] give $t_5(B_4)$ and $t_6(B_4)$. This gives the corresponding values for $a_k(B_3)$ and $a_k(B_4)$.

(3) Suppose $n > 4$ and $k < n$. In [22], Lin showed that any transitive homomorphism $B_n \to S_k$ has cyclic image. This implies $t_k(B_n) = (k-1)!$, and so $a_k(B_n) = 1$.

(4) In [1], Artin computed $|\mathrm{Epi}(B_n, S_n)|$ for all n. This gives $a_5(B_5) = 6$, $a_6(B_6) = 13$, and $a_n(B_n) = n + 1$, for $n > 6$.

(5) Suppose $6 < n < k < 2n$. In Theorem F.a) from [24], Lin proves that any transitive homomorphism $B_n \to S_k$ has cyclic image. Consequently, $t_k(B_n) = (k-1)!$ and so $a_k(B_n) = 1$.

(6) Suppose $n > 6$. Up to conjugation, there are 4 transitive homomorphisms $B_n \to S_{2n}$, of which 3 are non-cyclic, see [24, Theorem F.b)]. It is readily seen that the centralizer of those 3 homomorphisms is the involution $(1, 2)(3, 4) \cdots (2n-1, 2n)$. Hence, $t_{2n}(B_n) = (2n-1)! + 3(2n)!/2$, and so $a_{2n}(B_n) = 3n + 1$.

(7) Further results from Sections 4 and 7 in [24] give $t_6(B_5)$, $t_7(B_5)$, and $t_k(B_6)$, for $7 \leq k \leq 10$; the corresponding values for $a_k(B_n)$ follow.

Out of this discussion, we obtain the following corollary.

Corollary 10.5 *For the specified values of k and n, the number of index k subgroups of the braid group B_n is given by*

$$
a_k(B_n) = \begin{cases} 1 & \text{for } k < n \text{ and } n > 4, \text{ or } 6 < n < k < 2n, \\ n + 1 & \text{if } k = n \text{ and } n > 6, \\ 3n + 1 & \text{if } k = 2n \text{ and } n > 6. \end{cases}
$$

27

Based on this evidence, we propose the following conjecture.

Conjecture 1 *For all $n \gg 0$,*

$$a_k(B_n) = \begin{cases} 1 & \text{if } n \nmid k, \\ c(k/n) \cdot n + 1 & \text{if } n \mid k \end{cases}$$

where $c(k/n)$ is a constant, depending only on k/n.

Acknowledgements

References

[1]   E. Artin, *Braids and permutations*, Ann. of Math. **48** (1947), 643–649.

[2]   M. Aschbacher, R. Guralnick, *Some applications of the first cohomology group*, J. Algebra **90** (1984), 446–460.

[3]   G. Baumslag, *Groups with the same lower central sequence as a relatively free group. II. Properties*, Trans. Amer. Math. Soc. **142** (1969), 507–538.

[4]   G. Baumslag, D. Solitar, *Some two-generator one-relator non-Hopfian groups*, Bull. Amer. Math. Soc. **68** (1962), 199–201.

[5]   K. S. Brown, *Cohomology of groups*, Corrected reprint of the 1982 original, Grad. Texts in Math., vol. 87. Springer-Verlag, New York, 1994.

[6]   A. M. Cohen, L. Paris, *On a theorem of Artin*, J. Group Theory **6** (2003), 421–441.

[7]   E. Detomi, A. Lucchini, *Crowns and factorization of the probabilistic zeta function of a finite group*, J. Algebra **265** (2003), 651–668.

[8]   R. H. Fox, *Free differential calculus. III. Subgroups*, Ann. of Math. **64** (1956), 407–419.

[9]   R. H. Fox, *Metacyclic invariants of knots and links*, Canad. J. Math. **22** (1970), 193–201.

[10]   The GAP Group, *GAP–Groups, Algorithms, and Programming, Version 4.4* (2004); available at `http://www.gap-system.org`.

[11]   W. Gaschütz, *Die Eulersche Funktion endlicher auflösbarer Gruppen*, Illinois J. Math. **3** (1959), 469–476.

[12]   N. Gilbert, J. Howie, V. Metaftsis, E. Raptis, *Tree actions of automorphism groups*, J. Group Theory **3** (2000), 213–223.

[13]   E. A. Gorin, V. Ja. Lin, *Algebraic equations with continuous coefficients, and certain questions of the algebraic theory of braids*, Mat. Sb. **78** (1969), 579–610.

[14]   M. Hall, *Subgroups of finite index in free groups*, Canad. J. Math **1** (1949), 187–190.

[15]   P. Hall, *The Eulerian functions of a group*, Quart. J. Math **7** (1936), 134–151.

[16]   J. Hillman, *Alexander ideals of links*, Lecture Notes in Math., vol. 895, Springer-Verlag, Berlin-New York, 1981.

[17]   P. J. Hilton, U. Stammbach, *A course in homological algebra*, Second edition, Grad Texts in Math., vol. 4, Springer-Verlag, New York, 1997.

[18]   C. Kratzer, J. Thévenaz, *Fonction de Möbius d'un groupe fini et anneau de Burnside*, Comment. Math. Helv. **59** (1984), 425–438.

[19]   J. H. Kwak, J. Lee, *Distribution of branched D_p-coverings of surfaces*, Discrete Math. **183** (1998), 193–212.

[20]   J. H. Kwak, J.-H. Chun, J. Lee, *Enumeration of regular graph coverings having finite abelian covering transformation groups*, SIAM J. Discrete Math. **11** (1998), 273–285.

[21]   R. Lewis, S. Liriano, *Isomorphism classes and derived series of certain almost-free groups*, Experiment. Math. **3** (1994), no. 3, 255–258.

[22]   V. Ja. Lin, *Artin braids and related groups and spaces*, Algebra. Topology. Geometry, Vol. 17, pp. 159–227, 308, Akad. Nauk SSSR, Vsesoyuz. Inst. Nauchn. i Tekhn. Informatsii, Moscow, 1979.

[23]   V. Ja. Lin, *Configuration spaces of $\mathbb{C}$ and $\mathbb{CP}^1$: analytic properties*, `math.AG/0403120`.

[24]   V. Ja. Lin, *Braids and permutations*, `math.GR/0404528`.

[25] A. Lubotzky, D. Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser Verlag, Basel, 2003.

[26] D. Matei, A. Suciu, *Hall invariants, homology of subgroups, and characteristic varieties*, Int. Math. Res. Notices, **2002:9** (2002), 465–503.

[27] D. Moldavanski, *On the isomorphisms of Baumslag-Solitar groups*, Ukrain. Mat. Zh. 43 (1991), no. 12, 1684–1686.

[28] D. Moldavanski, N. Sibyakova, *On the finite images of some one-relator groups*, Proc. Amer. Math. Soc. **123** (1995), no. 7, 2017–2020.

[29] D. Robinson, *A course in the theory of groups*, Grad. Texts in Math., vol. 80, Springer-Verlag, New York, 1996.

[30] R. Strebel, *Homological methods applied to the derived series of groups*, Comment. Math. Helv. **49** (1974), 302–332.